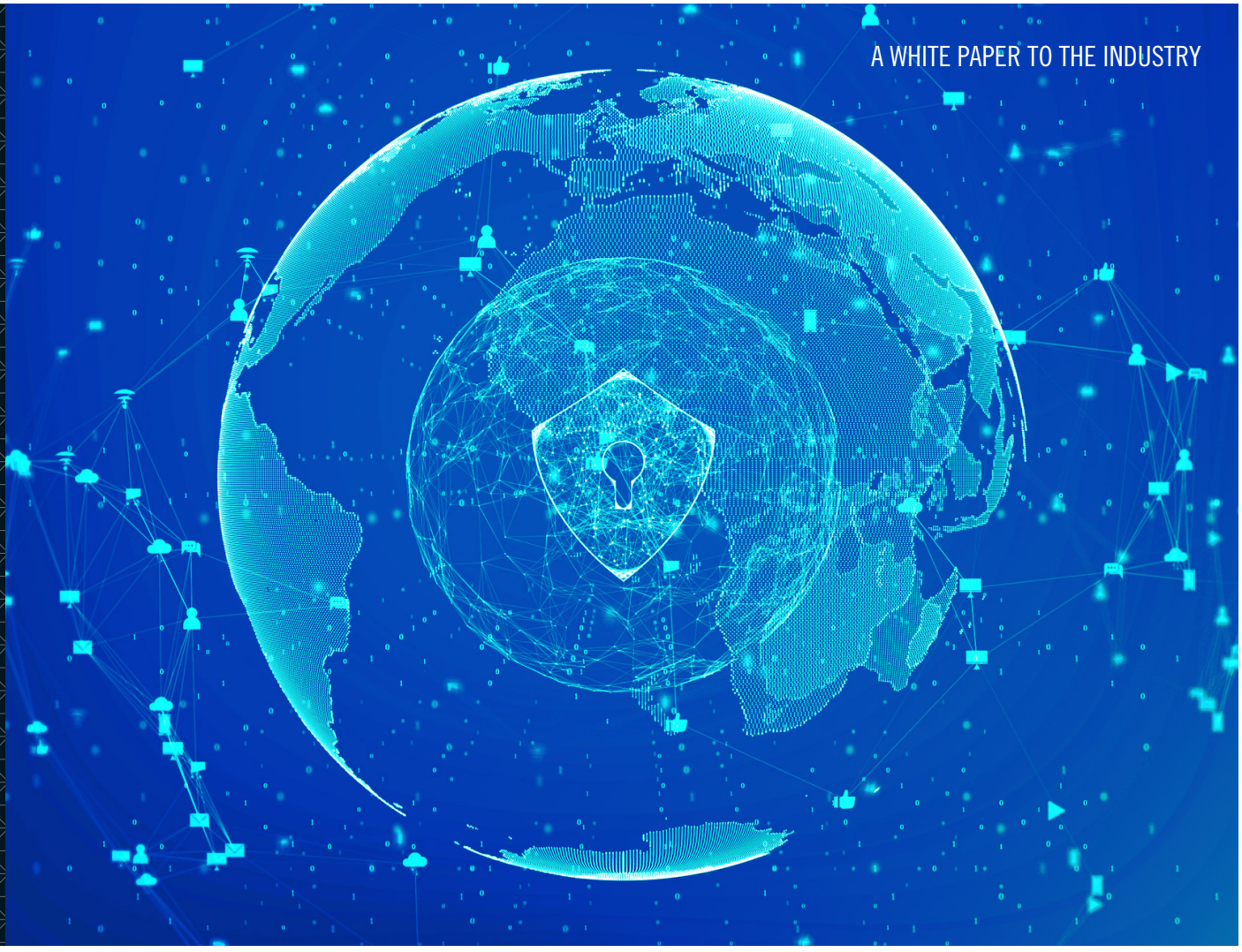
DTCC

Securing Today. Shaping Tomorrow.®

MARCH 2019

GUIDING PRINCIPLES FOR THE POST-TRADE PROCESSING OF TOKENIZED SECURITIES



Contents

EXECUTIVE SUMMARY

Markets for the trading of security tokens – tokenized representations of securities that are used to raise capital for various projects and initiatives – and of other "crypto assets" are growing rapidly in the U.S. and globally, creating a need for safe, secure and reliable post-trade processing of these transactions.

Distributed ledger technology (DLT) such as blockchain can be employed to effectuate the trading and/or post-trade processing of security tokens, on platforms referred to in this paper as Security Token Platforms. DLT has characteristics that are distinct from how traditional securities trading and post-trade processing platforms operate, thereby presenting challenges for regulators and market participants who seek to construct appropriate rules and structures for post-trade processing.

DLT-based Security Token Platforms can be designed in a variety of ways and may be either "permissionless" or "permissioned." By design, permissionless networks are unrestricted and have no defined governance structure to permit or vet their users; any entity with the requisite computer systems may participate in permissionless networks. Permissioned networks are restricted, allowing only those entities permitted to join the network to participate. Security Token Platforms can be configured for trading and/or settlement by combining permissionless and permissioned features, although involving a permissionless blockchain in the configuration will increase the complexity of the platform's operations and related policy considerations.

Existing regulations applicable to the post-trade processing of traditional securities should be applicable to the post-trade processing of tokenized securities. In some cases those existing regulations might not squarely apply.

In such cases, and because Security Token Platforms can be configured in a variety of ways, policymakers should take a functional approach to the features of a Security Token Platform. That is, those developing policy should determine the legal and other requirements applicable to a Security Token Platform based on the functions it performs and the risks it poses. These risks include custody risk, principal risk, and operational risk.

Regulatory principles developed by international standard setting bodies, such as the "Principles for financial market infrastructures," or PFMIs, can serve as useful guidance. These principles can help stakeholders in a Security Token Platform identify the types of post-trade responsibilities that should be applicable to a Security Token Platform that provides post-trade services. *(See the Appendix for discussion of the current framework for clearance and settlement of traditional securities.)*

The following post-trade responsibilities, which derive from specific, relevant international standards as well as regulatory requirements in the U.S. and around the world, should be undertaken by any platform providing post-trade processing of security tokens or other crypto assets:

- **DEMONSTRABLE LEGAL BASIS**
- **IDENTIFIABLE GOVERNANCE STRUCTURE**
- **IDENTIFIABLE RISK MANAGEMENT PROCEDURES AND SYSTEMS**
- **IDENTIFIABLE PROCEDURES AND SYSTEMS TO ENSURE SETTLEMENT FINALITY**
- **SECURITY TOKEN ISSUANCE, CUSTODY AND ASSET SERVICING**
- **RESILIENCE**
- **RECORDKEEPING REQUIREMENTS**

Promulgation and enforcement of these post-trade processing responsibilities will help enable Security Token Platforms to operate in a manner consistent with the public interest and foster the trust and confidence of investors.

INTRODUCTION

The Depository Trust & Clearing Corporation (DTCC) issued a white paper in 2016 to share its knowledge and insights on the applicability and challenges as well as potential opportunities of distributed ledger technology (DLT) systems, including blockchain, for the securities industry, particularly in the U.S.

Much has happened since then regarding DLT and blockchain. Open source projects such as Hyperledger[1] have been endeavoring to drive standardization in "permissioned" blockchain-based distributed ledgers.[2] Firms across the financial services industry have tested use cases for permissioned blockchains. DTCC initiated a project to re-platform its Trade Information Warehouse business onto a permissioned blockchain-based technology platform.

Additionally, the world has seen the emergence of various crypto asset tokens,[3] many of which are based on "permissionless"[4] blockchain networks such as Ethereum. A variety of assets have been tokenized using these networks with the goal of streamlining the process for exchanging the assets, including how transactions are booked and accounted for. One example of such tokenized assets is "security tokens," which have been used to raise capital for various projects and initiatives through offerings that are commonly referred to as initial coin offerings, or ICOs. For purposes of this paper, a security token is a tokenized representation of a security, as defined under the U.S. securities laws and subsequent case law.

SECURITY TOKEN PLATFORMS

- DLT such as blockchain can be employed to effectuate the trading and/or post-trade processing of security tokens, on platforms referred to in this paper as Security Token Platforms.
- DLT-based Security Token Platforms can be designed in a variety of ways and may be either "permissionless" or "permissioned."

PERMISSIONED BLOCKCHAIN

- A "permissioned" blockchain system is one that is private, closed or restricted, whereby central authorities control which entities are permitted to join the network to participate.

PERMISSIONLESS BLOCKCHAIN

- A "permissionless" blockchain system is one that is public, open and unrestricted, in which any entity with the requisite computer systems may participate.

These and other crypto assets can be traded on a variety of trading platforms around the globe. Some jurisdictions have established regulatory frameworks that trading platforms providing markets for crypto assets must adhere to. Others in the crypto asset space have established entities that would operate as "self-regulatory organizations" to establish best practices and rules for market participants to follow.

PURPOSE OF THIS WHITE PAPER

DTCC believes it is now time to consider guiding principles (for regulators and market participants) for the post-trade processing of crypto assets, to ensure that risks inherent in this process are identified, understood, and managed. Potential harms include those arising from custody risk (the loss of an investor's crypto asset), principal risk (for example, if a seller irrevocably delivers a crypto asset but does not receive payment) and operational risk (for example, the inability of an investor to access its crypto assets). Having been in the post-trade processing space for many years, DTCC has had a firsthand view of all the technological and regulatory changes over that time and also been intimately involved in many of those changes. As a result, DTCC believes it is in a unique position to contribute to the discussion in this area.

This paper focuses on the post-trade processing of crypto assets that are security tokens,[5] where the post-trade processing involves DLT, regardless of whether that processing is vertically or horizontally integrated with the trading platform.[6] This paper takes no position on the propriety of security tokens. However, since there is already demonstrable interest in such assets, this paper suggests that function-based guiding principles for post-trade processing of security tokens are in the interest of investors and other market participants.

While this paper does not discuss policy issues related to the actual trading of or environment provided for crypto assets or security tokens, if a crypto asset or security token meets the definition of a security under a particular jurisdiction's laws, DTCC believes that asset or token should be traded on a regulated trading platform.[7]

Instead, this paper focuses on the responsibilities that should apply to a platform that provides or is otherwise responsible for and involved in the process of completing trades in security tokens (post-trade processing), which we define here as a Security Token Platform. As suggested above, DTCC believes this discussion is highly relevant to policy considerations related to the post-trade processing of any type of crypto asset, or even derivatives on crypto assets, but the emphasis here is on the processing of security tokens.[8]

Because Security Token Platforms can be structured in a variety of ways, which may or may not be similar to structures of existing market infrastructures, this paper suggests that regulators adopt a functional approach to the regulation of Security Token Platforms. For example, DTCC is aware of platforms that have positioned themselves as both the trading platform for security tokens as well as the entity that would complete such trades.[9] DTCC suggests that regulators determine the legal and other requirements applicable to a Security Token Platform based on the functions it performs, and the risks posed by such Security Token Platform.[10]

If a Security Token Platform performs the same or a substantially equivalent function as an existing market infrastructure, thus exposing investors and other market participants to the same type of risk, the legal and other requirements applicable to that function should be the same regardless of whether the function is being performed by an existing market infrastructure or as part of a Security Token Platform.

When existing regulations do not apply, this paper suggests that regulators adopt a functional approach to the regulation of Security Token Platforms.

As described in more detail below, in the case of existing market infrastructures, such risk-based requirements include those under the Principles for financial market infrastructures (PFMIs).[11] This paper sets forth several of the PFMIs applicable to existing market infrastructures and addresses how regulators might consider applying such PFMIs to a Security Token Platform based on the functions it performs.

DTCC believes that unless these requirements are applied to Security Token Platforms – whether or not they are operationally vertically integrated with the trading platform – and are appropriately enforced under applicable law, a Security Token Platform would not operate in a manner consistent with the public interest. Moreover, DTCC believes that a Security Token Platform will not attract institutional investors unless these requirements are adequately met.

DISTRIBUTED LEDGER TECHNOLOGY, BLOCKCHAINS, AND CONFIGURATION OF SECURITY TOKEN PLATFORM

Distributed Ledger Technology (DLT) is generally described as follows:

> **"[a] distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network."[12]**

A blockchain structure is one form of DLT and, in this paper, the discussion assumes that the Security Token Platform utilizes a blockchain system in some fashion to perform trading and/or settlement services.[13] It is important to note that some Security Token Platforms might use non-DLT technology to run the trading systems and even the settlement services within a closed, vertically integrated ecosystem, but might nonetheless still reference ownership of the security in a blockchain, whether it be permissioned or permissionless.[14]

In a typical DLT structure, each transaction is verified by participants in the network. Once the relevant participants agree (generally through consensus-based validation protocols) on the details of the transaction, that transaction is cryptographically encoded and packaged into a new "block" and the new block is broadcast to other nodes on the network. In the blockchain structure each block is connected to the block established before it, creating a "chain." Most DLT networks are designed to minimize the possibility that the chain of blocks can be altered.[15]

Each participant on the network applies its computer to run certain algorithms and maintain a copy of the ledger. Each participant's computer that maintains the ledger is referred to as a **node.** In this paper DTCC assumes all information is distributed to each node in a network. Other networks may use a single central server, or a smaller group of validator nodes, to process and maintain information and distribute that information to the participants.

A significant component of a DLT platform is the potential use of **smart contracts.** Smart contracts are self-executing code. For example, in a Security Token Platform, a smart contract could potentially set forth the automatic procedures and processes for executing a transaction. Smart contracts could also potentially be used to facilitate payments, dividends, corporate actions, voting, notices, investors' tax status, etc. As further discussed in "Enforcement of Legal Orders and Smart Contracts" below, the term "smart contract" is often a misnomer, in that the self-executing code may not be a legally enforceable contract in the relevant jurisdiction: it depends on the nature of the smart contract, the underlying DLT platform, its operating procedures and the legal framework in the relevant jurisdiction.

There are two basic types of DLT networks: **permissionless** and **permissioned.**[16]

PERMISSIONLESS NETWORKS

For purposes of this paper, in a permissionless network, anyone and everyone could join if they choose and every network user is allowed to contribute to it, adding transactions to the ledger. A key feature of these permissionless networks is that, by design, they have no governance structure to permit or vet their users. Because the identities of their users and contributors are unknown, users have not been qualified through any type of anti-money laundering, know-your-customer, or OFAC process.[17]

Other features of permissionless networks include:

- Nodes may be located in any part of the world.
- Information generally can be validated by anyone who chooses to be on the network through a consensus protocol.
- Governance is generally accomplished through consensus.
- Consensus is the method by which nodes on the network determine whether certain actions have taken place. As a result, no single legal entity is responsible for governance decisions, record keeping, or dispute resolution.

Because of their dependence on achieving consensus, permissionless networks may be hindered in addressing challenges posed by unforeseen events and changes to the markets, market infrastructures, and the technology platform that could require modifying the software or the network. In many cases permissionless networks include foundations that continue to develop the DLT networks and underlying protocols (the Ethereum Foundation is a good example).

PERMISSIONED NETWORKS

In a permissioned network, access is restricted to approved participants. A permissioned network provides a model to restrict participation to trusted entities. Further, certain participants may have different levels of access depending on the structure created by the network operator. Participants may be granted access to one or more of the following: (i) the right to read the ledger, (ii) the ability to initiate transactions, or (iii) the ability to update the ledger/validate transactions.

A permissioned network allows for a centralized governance structure and enables assignment of responsibilities to a network operator. Decision-making may be more centralized for certain aspects of the network and more distributed for other aspects.[18]

As discussed more fully below, some Security Token Platforms involve both permissionless and permissioned networks for the settlement of a single transaction.[19]

DEVELOPMENT AND CONFIGURATION OF SECURITY TOKEN PLATFORMS

How a tokenized security trades and settles on a Security Token Platform will depend on the structural choices made by the platform developer. There will be hundreds if not thousands of DLT platforms, with each one potentially structured in a different way. Given the potential variability of DLT platforms and networks, the structure and functions of a particular Security Token Platform would need to be fully understood in order to evaluate it from both a policy and legal perspective.

In some cases, a Security Token Platform may be configured such that settlement of the security token involves a public blockchain, even if the trading activity itself is contained within a permissioned system. Different models of configuration involving permissionless and permissioned networks may be combined to provide viable platforms for trading and settlement. Importantly, involving a permissionless blockchain in the configuration will increase the complexity of the platform's operations as well as the policy considerations involved.

For instance, for tokens created on the permissionless Ethereum network pursuant to the ERC-20 protocol (the technical standard for smart contracts on the Ethereum network), only Ether can be used to purchase them. (Ether is the only intra-platform currency on the Ethereum blockchain network.) If implemented in compliance with applicable securities laws, i) ownership of this type of token would be reflected in the Ethereum blockchain and, ii) arguably, the transaction involving the security token would be completed only once the transaction involving Ether was completed (i.e., the security token is delivered versus payment of Ether).

In this type of system, the settlement process is complex because of considerations regarding transaction finality on the Ethereum network. Furthermore, meeting the post-trade responsibilities advocated later in this paper would be difficult, due to uncertainties about whether any protocol for tokenizing assets on a permissionless blockchain such as ERC-20 are acceptable.

HYPOTHETICAL DLT TRADE

Below is a high-level description of a hypothetical securities trade executed on a Security Token Platform. Because Security Token Platforms can be designed in various ways, the following is only one example:

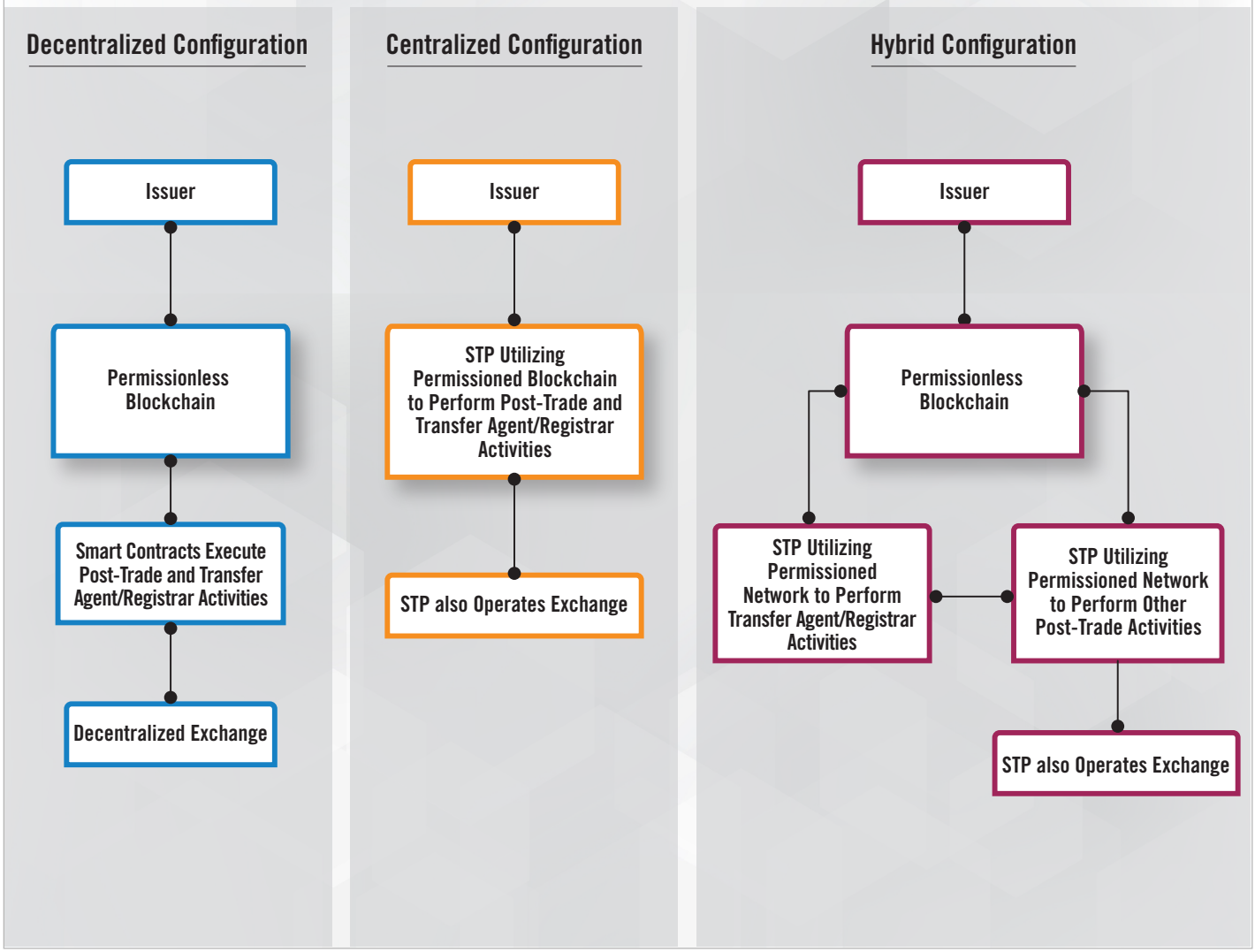
Each security on the Security Token Platform would be defined through a smart contract and represented by a token issued by the related issuer. The issuer would control the outstanding tokens to the same extent it controls its existing outstanding securities. A token, once issued and purchased, would be held in a purchaser's or owner's wallet.

Each investor has a "cash ledger" and a "securities ledger" relating to this particular Security Token Platform.[1] The investor's cash ledger and securities ledger can be linked to an account or "wallet."

Two investors agree on a trade. Each proves that it has either the required cash (or other digital or crypto currency) or securities to conduct the trade. The seller's securities ledger is debited the security sold, and the buyer's cash ledger is debited the sales price. The buyer "posts" its "cash" (i.e., the buyer transfers from a wallet digitized cash) and the seller "posts" its securities (i.e., the seller transfers from a wallet tokenized securities) to the Security Token Platform and each signs with its private key to verify its identify and execute the trade. The proposed trade is broadcast to the nodes on the network to be verified (through consensus mechanism). Once verified, a new block is created identifying the trade, the buyer's wallet is credited with the securities, and the seller's wallet is credited with cash.

1 See Slaughter and May & Euroclear, Blockchain Settlement, Regulation, Innovation and Application (2016).

Three Basic Configurations for Security Token Platforms (STP)



SUGGESTED POLICY AND LEGAL FRAMEWORK FOR POST-TRADE PROCESSING OF CRYPTO ASSETS

CURRENT LEGAL FRAMEWORK FOR CASH EQUITIES CLEARANCE AND SETTLEMENT

Jurisdictions around the world have taken substantially similar approaches to assigning and enforcing responsibilities to those entities providing post-trade processing for cash equities. This was true before the financial crisis of 2008 but has become even more so since then, in part because of the development of the Principles for financial market infrastructures, or PFMIs, and their use by national jurisdictions as the foundation for local rules and regulations. As mentioned, U.S. and international regulators utilize the PFMIs – a comprehensive and widely-used set of principles – to assess central securities depositories (CSD), securities settlement systems (SSS), central counterparties (CCP), systemically important payment systems (PS) and trade repositories (TR).[20]

The PFMIs can help interested parties identify and understand the types of post-trade responsibilities that might be applicable to a Security Token Platform that also provides post-trade services. However, not all of these responsibilities may be relevant, feasible or important in a Security Token Platform environment.

It is possible to design a Security Token Platform configured to involve a permissionless blockchain that provides some of the functions in support of a trusted, regulated financial market infrastructure (FMI) acting as a central authority. However, assigning and enforcing the responsibilities discussed below would be difficult without reconsidering policy requirements or redesigning the attributes of permissionless networks – in part because requirements, such as those for smart contracts, are continually evolving.

Security Token Platforms should have a sound, clear and enforceable legal basis for its structure.

Short of applying relevant regulation applicable to securities processing, DTCC believes that borrowing from the PFMI would require that any Security Token Platform should have a sound, clear and enforceable legal basis for its structure. Ambiguity or a lack of certainty will increase legal risks[21] and operational risks for the platform. To the extent that such a platform eliminates or, more likely, integrates one or more steps that exist in the current system, stakeholders will need a clear understanding of how the platform functions, the rights and obligations of each participant, and how those rights and obligations are set forth in legal, enforceable contracts.

Given the numerous potential configurations of a Security Token Platform, infrastructure principles should also be used to assess any Security Token Platform or crypto asset platform.

DTCC believes any platform that provides post-trade processing of security tokens should bear the following post-trade responsibilities. DTCC believes that these responsibilities are also applicable or highly relevant to most crypto assets. These responsibilities derive from specific, relevant international standards as well as specific regulatory requirements in the U.S. and elsewhere:

- Demonstrable Legal Basis
- Identifiable Governance Structure
- Identifiable Risk Management Procedures and Systems
- Identifiable Procedures and Systems to Ensure Settlement Finality
- Security Token Issuance, Custody and Asset Servicing
- Resilience
- Recordkeeping Requirements

DEMONSTRABLE LEGAL BASIS[22]

DTCC believes it is critical to identify the law that would best apply to the activities and user relationships of a Security Token Platform. A Security Token Platform should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

With a Security Token Platform utilizing a permissionless blockchain network – whereby any user can add a node to the network – the mechanisms by which a platform would adopt a choice of governing law, as well as how such choice would be agreed to and enforced, are unclear. Because a node on the permissionless network could be located anywhere in the world, the degree to which the governing law would be enforceable may need complex legal logic covering every regional policy to be built into every smart contract and depend on the location of the nodes. For example, even when the Security Token Platform utilizing a permissionless network is governed by the laws of a particular jurisdiction, if a majority of the nodes are located in jurisdictions that would not recognize such laws (or, even more fundamentally, the legal effect of transactions processed on such platform), the platform effectively would not be governed by the law the parties had agreed to.

In a Security Token Platform utilizing a permissioned blockchain network, some of these issues could be managed by the central authority overseeing the platform. While the degree to which the choice of governing law is enforceable against a party depends on where the party is located, where the token is located, or where the token issuer is located, in a Security Token Platform utilizing a permissioned network, the legal risk associated with foreign parties can be flagged and mitigated in advance. In appropriate circumstances, a foreign node could even be restricted or eliminated from participating in the platform (other than perhaps on a read-only basis) if its participation presented material legal risk to the platform, as deemed by the central authority. Additionally, the customized smart contract and data distribution models available in permissioned networks can be tailored to the specific requirements of transaction parties and participating nodes.

REGISTRATION OF SECURITY TOKENS

At the state level in the U.S., Article 8 of the Uniform Commercial Code (Article 8) governs how interests in securities are evidenced, how they are transferred in the current securities market, and the rights and duties of those who are involved in the transfer process. Under U.S. state law, the law of the issuer's jurisdiction (or, if permissible, another law specified by the issuer) governs the effectiveness of the issuance of a security.[23] Therefore, if securities are to be created and exist solely through a distributed ledger, it will be incumbent on the securities issuer to ensure the applicable law is compatible with the operation of the Security Token Platform and that ownership transfers on the distributed ledger have legal effect in such jurisdiction. For example, in 2017 Delaware amended its General Corporation Law to explicitly allow Delaware corporations to use DLT to maintain corporate records, including the corporation's stock ledger.[24] Many other U.S. states have enacted or proposed similar laws.[25]

ENFORCEMENT OF LEGAL ORDERS AND SMART CONTRACTS

In a Security Token Platform, utilizing a permissionless blockchain network, there is risk that a court of competent jurisdiction could order and effect legally mandated changes to the distributed ledger, such as in the context of probate or divorce proceedings, when affected users may be unable or unwilling to effect such changes directly, thus preventing or frustrating the enforcement of law. In a permissionless configuration, the same issue would apply to orders from regulators imposing restrictions on the platform's operation, such as trading suspensions.

In a Security Token Platform utilizing a permissioned blockchain network, the central authority overseeing the platform would presumably have a transparent administrative process to effect legally mandated orders; otherwise such automated functionality may need to be included in the platform to ensure compliance with such orders.

A related matter for a Security Token Platform utilizing a permissionless network is the degree to which a node would be subject to jurisdiction outside its home jurisdiction. An inability to exercise regulatory authority over a foreign node would impede a regulator's ability to enforce the laws and regulations they are charged with enforcing. For example, in the case of a Security Token Platform utilizing a permissionless network, it may be impossible to enforce a regulator's trading suspension in respect of a security if a substantial number of the nodes are not subject to that regulatory jurisdiction. This challenge is compounded if multiple government-sponsored supervisors assert jurisdiction based on the fact that nodes, and associated transaction data from participants in the permissionless network, are located in multiple jurisdictions.

Another consideration is the degree to which other entities or organizations that can affect operations of the Security Token Platform – for example, platform developers and/or foundations that can propose alterations to existing code or the standards underlying the platform – are subject to the exercise of a regulator's authority. When such entities are beyond the reach of relevant regulators, such an arrangement could present material legal risk to the operation of the platform and the ability of regulators to oversee its operation consistent with their regulatory mandate.

Smart contracts raise various enforceability issues – for one, as smart contracts are written purely in code (raising the question of whether such contracts are discoverable by both parties and thus whether a "meeting of the minds" has occurred), can these contracts instead be written in both code and in writing? Even straightforward smart contract code may require thousands of lines of computer logic with associated conditional operations and loops, etc. More complex contracts may be much larger. Code defects and unexpected consequences are also likely for more complex constructs.

Additionally, the degree to which business logic is built into a Security Token Platform implementing smart contracts while leaving other portions of the logic "off-chain" in legacy systems, could further complicate discoverability and common understanding. A Security Token Platform utilizing a permissionless blockchain network also raises questions concerning smart contracts' performance – for example, how, and by what means, it is possible to reform or modify a smart contract in the event of changed circumstances such as an issuer merger or bankruptcy.

IDENTIFIABLE GOVERNANCE STRUCTURE[26]

A Security Token Platform should have appropriate governance arrangements to support its operation, including effective rules regarding functionality and risk management. The governance structure will largely depend on whether the platform is utilizing a permissionless or permissioned network, or implements some combination of the two.

GOVERNANCE OF SECURITY TOKEN PLATFORMS UTILIZING PERMISSIONLESS NETWORKS

As discussed above, a Security Token Platform utilizing a permissionless blockchain network uses a consensus mechanism among the network nodes to make significant platform changes. There is no central authority in the traditional sense to deal with functionality changes, unexpected consequences of network design decisions or externalities such as changes to the regulatory environment or external attacks on the network.[27]

In a permissionless network, node operators are untrusted and not legally bound to each other, but are expected to operate in the best interest of the network solely because of the built-in incentive models (e.g., bitcoin mining payments). In the absence of a central authority, it is the operators of the nodes who must determine what, if any, response (such as a change to the underlying code) is appropriate when something improper or unexpected occurs regarding the Security Token Platform.

A Security Token Platform should have appropriate governance arrangements to support its operation, including effective rules regarding functionality and risk management.

It is more difficult to correct mistakes or other errors in the case of a Security Token Platform utilizing a permissionless network as it might require node operators to reach consensus on the appropriate error correction. While one of the goals of a distributed ledger is to ensure its immutability and stability, the ability of traditional FMIs and market participants to correct errors prior to settlement (such as the cancellation or offset of erroneous trades) has proven useful to equities markets.

And on a Security Token Platform utilizing a permissionless network, it is not clear the degree to which node operators have legal obligations to other platform participants, such as a duty to continue platform operations or attempt to remedy (or not exploit) discovered platform vulnerabilities.

GOVERNANCE OF SECURITY TOKEN PLATFORMS UTILIZING PERMISSIONED NETWORKS

Because Security Token Platforms utilizing permissioned networks allow for centralized governance, they should be more adaptable than platforms utilizing permissionless networks to the current regulatory environment for securities clearance and settlement, or to otherwise assign post-trade responsibilities.

A Security Token Platform utilizing a permissioned network may also allow mistakes or other errors on the distributed ledger to be corrected by a central authority. However, the ability to correct mistakes and errors carries risks: if transactions can be reversed, it is harder to ensure they will become final and settle as expected. A preferred model should support the immutable ledger and audit log ethos of the blockchain and allow the central authority to add transparent correcting transactions without changing previous history. The central authority's ability to unwind transactions – including the movements of securities and cash – following settlement also creates risk to market participants. For details, see the discussion of "Identifiable Procedures and Systems to Ensure Settlement Finality" below.

It is generally assumed that Security Token Platforms will provide RTGS and thus reduce settlement time as well as credit risk and liquidity risk from the platforms and their users.

To mitigate these risks, protocols should be in place – including oversight of the central authority by platform participants and/or external regulators – to determine if and when error correction by the central authority is appropriate. The central authority may also want, or be required, to have some way to enforce legal orders.

If the central authority is empowered to make changes to the Security Token Platform, regulators might deem it to be engaging in regulated activities within the meaning of local laws – in which case the relevant regulators would need to determine the central authority's appropriate regulatory status given the applicable facts and circumstances.

IDENTIFIABLE RISK MANAGEMENT PROCEDURES AND SYSTEMS[28]

A Security Token Platform, depending on its structure, can present different types and levels of risk and other externalities to itself and its users. No matter its structure, a Security Token Platform should have a sound framework for comprehensively managing legal, credit, liquidity, operational, and other risks.[29]

To the extent that a Security Token Platform reduces trade settlement time, it has the effect of shortening the time period during which a trade counterparty could potentially default, thus reducing credit risk and liquidity risk. In the case of real-time gross settlement (RTGS) systems, where both the securities transfer and payment transfer settle immediately in real time, reducing settlement time to zero correspondingly lowers credit risk and liquidity risk to zero. However, the risk reduction of RTGS systems is not cost-free because it requires participants to keep sufficient liquid assets on hand in order to be able to settle their transactions in real time. This liquidity ties up assets that could be used for other purposes, unless an RTGS system is designed to allow automated real-time access to the platform for participants' credit providers, which of course would create a different channel of credit risk.

RTGS systems differ from the netting systems of some traditional FMIs, such as DTC and NSCC, where securities and payment obligations are offset to reduce the number and value of payments and deliveries needed to settle a set of transactions. While netting significantly reduces the degree to which system participants need to tie up liquid assets in order to settle transactions, it correspondingly exposes those participants, and the system itself, to the credit risk and liquidity risk posed by deferring settlement.

It is generally assumed that Security Token Platforms will provide RTGS and thus reduce settlement time as well as credit risk and liquidity risk from the platforms and their users. But such reductions will impose tremendous cost on users by requiring them to pre-fund their trading activities or obtain real-time access to credit facilities integrated into the platforms. This situation would be particularly concerning to institutional investors who may need to tie up significantly greater amounts of liquidity in an RTGS platform than in one that nets transactions. The concern is compounded when institutional investors need to separately ensure liquidity on numerous distinct DLT platforms.

Additionally, if a Security Token Platform assumes a critical role in effecting securities transactions as well as custody and asset servicing, the question arises as to whether the platform should have in place adequate measures to address possible unavailability or discontinuance of its activities.[30] The nature of these measures would depend on the structure and operations of the particular platform. For example, it is unclear whether the costs of a Security Token Platform configured to leverage a permissionless blockchain would or should include the operation of the permissionless network, which it does not control. The calculus would seem to change for a platform utilizing a permissioned network that is responsible for operating a central authority overseeing the platform. The extent to which the platform is subject to regulatory oversight would also likely influence the level of capital it needs, both in terms of regulatory capital requirements and ongoing legal and regulatory compliance.

IDENTIFIABLE PROCEDURES AND SYSTEMS TO ENSURE SETTLEMENT FINALITY[31]

Settlement finality is a critical concept in securities markets, including those for tokenized securities. Those who participate in securities markets hold justifiably high expectations regarding settlement. Generally, a Security Token Platform that provisions services to complete a trade should be expected to provide clear and certain final settlement.[32]

If an otherwise completed transaction is not final, it remains susceptible to being unwound in connection with, among other things, the bankruptcy or insolvency of a counterparty. It is easy to imagine the uncertainties and difficulties arising from an attempt to unwind an otherwise completed transaction. For example, what if one or more of the parties is no longer in possession of what it received or otherwise unable to return it? Or what if the two legs of a trade (e.g., a security and the cash it was purchased for) are no longer equivalent in value, subjecting one party to an unexpected loss? Brokers or agents that simultaneously buy and immediately sell the same security, which are paired off or netted in today's settlement systems, can potentially have one side or the other not complete and be exposed to enormous price risk.

OPERATIONAL FINALITY

It is important to financial markets that transactions be considered "final" at some point in time, to ensure they cannot be unwound. Because settlement finality means a transaction cannot be unwound, the point at which settlement becomes final is determined by both the rules of the market (operational finality) and the governing legal framework in the relevant jurisdiction (legal finality).

In the case of a Security Token Platform, especially one utilizing a permissionless network with a consensus mechanism to determine the state of the distributed ledger, it is unclear when settlement can be considered operationally final. It takes time to reach consensus and confirm a transaction. At a single point in time, the requisite number of nodes may not agree on the state of the ledger (e.g., because of simultaneous transaction processing by nodes and latency in communications between nodes), or an adequate number of blocks may not have confirmed a transaction.

The point at which settlement becomes final is determined by both the rules of the market (operational finality) and the governing legal framework in the relevant jurisdiction (legal finality).

As a result, whether final operational settlement has occurred may be, at best, probabilistic due to the difficulty of determining the point at which the transaction becomes final. To solve this problem, depending on the specific blockchain in use, policymakers could provide guidance on the minimum number of blocks needed to confirm a transaction before the settlement is considered final, thus providing legal finality on this point (see below).[33] With a Security Token Platform utilizing a permissionless blockchain network, nodes can also attempt to revise transactions previously confirmed by other nodes. The disagreement may result in creation of a "fork" – a bifurcation of the distributed ledger potentially resulting in two claims on the same asset.

These operational finality issues may pose less of a concern for Security Token Platforms using permissioned networks. Since all the nodes and users in a permissioned network are known and trusted, protocols used to create consensus are more definitive and can be enforced and made time-bound. The nodes and users in a Security Token Platform using a permissioned network would be required to contractually agree as to when a transaction is considered final or that a central authority (or defined subset of nodes or users) determines when a transaction is considered final. It may also be possible for nodes and users in a platform utilizing a permissioned network to use existing commercial law frameworks to define the point of settlement finality between themselves and with respect to third parties.[34]

LEGAL FINALITY

Unlike operational finality, legal finality in a Security Token Platform will depend on the legal framework for finality under applicable governing law and the legal and regulatory status of the platform's components. First it must be determined which governing law applies to the Security Token Platform (see the discussion above on "Demonstrable Legal Basis"). Legal insolvency regimes are important. In the United States, the U.S. Bankruptcy Code and other applicable U.S. insolvency regimes generally provide that a "securities contract," including an agreement to purchase or sell a security made by or to (among others) brokers, financial institutions and registered clearing agencies, may not be unwound and may not be stayed.[35] This legal framework enables transactions to reach legal finality in the regulated securities markets.

However, the extent to which this legal framework would apply to a Security Token Platform would depend on whether the securities contract was made by or to a regulated entity such as a broker, financial institution or registered clearing agency.[36]

FIAT/MONEY SETTLEMENT[37]

DTCC believes that whether the means of payment used presents unreasonable risk to the Security Token Platform and its underlying blockchain network is an important consideration. A Security Token Platform should ensure that, to the extent the obligation to deliver a security is linked to an obligation to make payment, settlement of one obligation should be conditioned upon settlement of the other obligation. Normally, a securities transfer and the payment transfer of a delivery versus payment (DVP) transaction settle simultaneously.

In order for the payment and securities transfers to settle at the same time, the securities market and the payment system must interact. In the current U.S. equities markets, DTC submits instructions to the Federal Reserve's National Settlement Service to effect net money settlement at the end of the business day for activities at DTC and NSCC. Other CSDs around the world use a similar set of procedures leveraging similar payments systems. The U.S. Federal Reserve's Fedwire Securities Service, in contrast, is linked on a real-time basis to master accounts at the Federal Reserve Banks, thus each transaction simultaneously debits/credits securities while crediting/debiting central bank money.[38]

Central banks including the Bank of Canada, Bank of England, and Sweden's central bank have undertaken initiatives to explore the feasibility of digitizing central bank money on a distributed ledger.

Depending on the legal and regulatory status of the components of a Security Token Platform, the platform may be able to directly access the government-sponsored payment system.[39]

If the platform cannot directly access a government-sponsored payment system, it may be able to use a commercial banking relationship to process payment activity on the system. However, the use of a commercial bank introduces risks to the platform, including credit risk and liquidity risk relating to funds held with the commercial bank, which the platform needs to manage.

For some Security Token Platforms, the settlement process might involve digital currencies. Any consideration of digital currencies, rather than government-issued currency, for payment on a Security Token Platform would entail a very different risk profile that would need to be managed by the platform and should be disclosed to the general public or market. While holding any currency entails some risk (such as deflation or inflation), the degree to which a digital currency acts as a stable store of value or medium of exchange would significantly affect the risk of utilizing such digital currency.

Central banks including the Bank of Canada, Bank of England, and Sweden's central bank have undertaken initiatives to explore the feasibility of digitizing central bank money on a distributed ledger, which would make it possible for Security Token Platforms to settle payments in central bank money. However, unless and until any networks of central bank digital currency become operational, the legal and regulatory burdens associated with participating in such networks cannot be fully ascertained.

EXCHANGE-OF-VALUE SETTLEMENT SYSTEMS[40]

Securities transactions involving the settlement of two linked obligations are expected to eliminate principal risk by the settling agent conditioning the final settlement of one obligation upon final settlement of the other. The same should be expected of a Security Token Platform: it should have procedures and systems to ensure that, if an obligation to deliver a security token is linked to an obligation to make payment (i.e., the security is delivered against payment), settlement of one obligation is conditioned upon settlement of the other obligation. As discussed, the Security Token Platform would be expected to settle the payment leg of transactions it effectuates in central bank money or, failing that, by using funds — digitized cash or otherwise — that do not present unreasonable risk to the platform.

In order to ensure DVP, there must be a link between the securities transfer and the payment transfer. Today in the U.S., DTC operates a deferred net settlement system, not an RTGS system, which means DVP securities transfers in the DTC/NSCC system are generally not final unless and until system-wide funds settlement has been completed.

There are several ways a Security Token Platform in an RTGS model could be able to offer DVP: through arrangements with existing FMIs such as Payment Systems (PS); through use of digital currencies; or with commercial bank platform users that supply credit to trading parties through a mechanism that interfaces with the commercial banks' central bank accounts. In the third scenario, a transaction for which a trading party has no funds available may still be completed if the party has credit available with a commercial bank and that bank has funds available in its central bank account that can be transferred to the trade counterparty's central bank account (or its credit provider's central bank account).

While separate distributed ledgers might be kept for securities and cash, one recent study by two central banks examined the degree to which both cash and securities could be recorded on the same distributed ledger.[41] The study determined that a securities platform with such a configuration could indeed eliminate principal risk by ensuring DVP.[42] To be viable, such a configuration would need to allow the cash recorded on the distributed ledger to be moved elsewhere. Accordingly, a Security Token Platform developer would have some flexibility in designing the platform to ensure DVP, including conversion from any native token (such as Ether) to cash.

A Security Token Platform should have procedures and systems to ensure that, if an obligation to deliver a security token is linked to an obligation to make payment (i.e., the security is delivered against payment), settlement of one obligation is conditioned upon settlement of the other obligation.

SECURITY TOKEN ISSUANCE, CUSTODY AND ASSET SERVICING[43]

This section of the paper is most relevant to Security Token Platforms that provide post-trade processing of security tokens. As with a CSD, a Security Token Platform (or one or more of its components) should have appropriate rules and procedures in place to help ensure the integrity of securities or security token issues and minimize and manage the risks associated with the safekeeping and transfer of securities for which the platform is responsible, regardless of whether it is treated as a CSD under the current legal framework.

Given that securities will be created and exist solely through a distributed ledger, the Security Token Platform should incorporate processes to authenticate and process securities issuances and redemptions. In the U.S. equities market, those duties are generally fulfilled by the issuer and its transfer agent rather than a CSD.

It is not clear how such processes would operate on a Security Token Platform. As indicated above, a Security Token Platform configuration might involve a network where the issuance, trading, custody, and asset-servicing of the security tokens all take place. Or the configuration might include a separate system for the issuance, custody and asset servicing of the security token. Or further still, it is conceivable that the configuration might include a separate system or platform that acts as the legal registrar but does not serve as a legal custodian for the tokens, similar to the functions of a transfer agent in the U.S.

In any case, at a minimum, the entity responsible for issuance, custody and asset servicing should interface with the issuer to determine whether securities need to be issued or redeemed. To provide the issuer the authority for issuing or redeeming securities requires giving the issuer that functionality and withholding that functionality from others on the platform. Implementing such functionality would be challenging on a Security Token Platform utilizing a permissionless blockchain network, but more feasible on a platform using a permissioned network.

RESPONSIBILITIES OF TRANSFER AGENT/REGISTRAR

Transfer agents act as agents for issuers, fulfilling a role that is distinct from CSDs. Generally, transfer agents record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends. In some marketplaces such as the U.S., they have a key role in the securities settlement process and may be subjected to regulatory obligations. It is conceivable that a Security Token Platform could fulfill the activities currently performed by transfer agents – even separate and apart from the platform where trading takes place – and therefore should be expected to bear certain responsibilities such as those laid out in regulations.

CUSTODY

It is of paramount importance that any securities-holding system adequately addresses custody risks. Custody risk is a bit unusual on a Security Token Platform. For security tokens that are traded and processed on such a platform, the securities are created and exist solely through the distributed ledger. Consequently, mitigating the platform's custody risk focuses on equipping the Security Token Platform to properly safeguard the securities on the platform rather than ensuring a custodian is properly physically safeguarding assets.

A Security Token Platform should have robust accounting practices, safekeeping procedures and internal controls that fully protect assets for which the platform is responsible – including wallet structures that allow assets to be segregated by user and from the assets of the platform itself. The platform should undertake an assessment of the legal basis of its custody measures, including its wallet structure.

To the extent a Security Token Platform also holds cash belonging to its users, the platform should hold such cash at adequately capitalized and regulated banking institutions, including central banks, that appropriately segregate such cash from the assets of the Security Token Platform. The cash should also be readily accessible by the Security Token Platform. While holding user cash at a commercial bank (as opposed to a central bank) exposes the platform to the

bank's credit and liquidity risks, if the bank is adequately capitalized and appropriately regulated the Security Token Platform is significantly less likely to suffer a loss on the deposit. A system designed to interface with the bank's account at the central bank further mitigates this risk.

ASSET SERVICING

Relatedly, a Security Token Platform should be able to facilitate asset servicing – including the processing and reporting of dividends and other distributions, shareholder voting and notices, shareholder lawsuits, and the processing of corporate actions such as stock splits and mergers – on the securities for which it is responsible. As described above, it may be possible for some asset servicing functions to be automated by smart contract. Any communications with holders would be expected to be paperless and holders would have an opportunity to receive notification of such events. The automated nature of a smart contract may eliminate some of the obligations of a registrar, transfer agent and/or exchange agent.

It is an open question who would be responsible for the functions automated by a smart contract, particularly if something goes wrong or there is a change in circumstances necessitating a change to the smart contract, and what would be the legal and regulatory status of such person. To the extent that certain asset servicing functions could not be automated by smart contract, such functions would need to be performed by persons with the appropriate legal and regulatory status to do so, but how such persons would interact with the Security Token Platform, especially in a permissionless network, is unclear.

RESILIENCE[44]

The resilience of market infrastructures involved in capital markets is of great concern to the policymaking and regulatory community, which in recent years has stepped up its analysis of rules and best practices to ensure they promote resilience.[45] The debate around resilience has intensified in part due to the growing threat of cyber-attacks from private and state actors.

Security Token Platforms should be expected to identify plausible sources of operational risk, internal and external, and mitigate their impact through appropriate policies, procedures, and controls and with systems designed to ensure a high degree of security and operational reliability and adequate, scalable capacity. Their controls should include business continuity plans that aim for timely recovery of operations and fulfillment of a platform's obligations, including in the event of a wide-scale or major disruption.

Domestic and international standards relating to cybersecurity also should be instructive regarding the resilience of Security Token Platforms.[46]

Operational risk is especially relevant for a Security Token Platform given the degree to which it requires seamless integration of various technological components and the significant impact its unavailability would have on users. Operational risk exists anywhere an operational failure or disruption could occur in the Security Token Platform. Operational failures, errors or delays in processing, errors in coding, fraud, data loss and leakage, system outages, demand exceeding capacity, and the relative strength of a platform's cryptography may lead to platform failures and result in significant monetary losses and a loss of confidence in the platform's safety and soundness. At a minimum, a Security Token Platform should be able to demonstrate that it can be operated safely and has a high degree of resiliency and security.

One operational risk of a Security Token Platform is its underlying operational capacity and scalability. Operational capacity should include (i) large volumes of data, and (ii) the ability to handle peak volumes, particularly in times of market stress. Cryptography, which is used to manage rights and access to data, is a core component as the level of encryption and the management of encryption keys are critical to managing the platform's operational risk. DLT platforms have been subject to attack and security threats are continually evolving. A Security Token Platform therefore should be organized to quickly adapt to new and emerging threats. While a distributed network may provide greater redundancies and, as a result, reduce the impact of a problem with any component of the network, such distribution would not eliminate all risk and may offer greater opportunity for attack.

Therefore, in addition to a risk management framework, it would be prudent for a Security Token Platform to have a business continuity plan in the event of a wide-scale or major disruption.

RECORDKEEPING REQUIREMENTS[47]

Robust recordkeeping practices are another important post-trade responsibility of market infrastructures. Smart contracts could be programed to maintain records and provide reports in various ways. Because DLT allows for data and records to be stored across multiple nodes, supervisory agencies could be provided with a node that effectively granted permanent read-only access to the platform's electronic records. However, whether nodes on a blockchain network utilized by a Security Token Platform would meet any given jurisdiction's recordkeeping requirements, including any immutable storage requirements, is an open question.

The smart contracts and related records should be structured to allow for third-party audit and for a designated third party to access, search, and produce such records. A Security Token Platform should demonstrate how it manages the privacy and confidentiality of appropriate records, particularly records that contain users' personal or proprietary information, while maintaining their accessibility to regulators and appropriate third parties such as external auditors.

A well-designed Security Token Platform could give supervisory staff greater access to real-time activity than is now possible. However, that same staff may be burdened with learning how to access a variety of Security Token Platforms, each with a potentially unique method of storing data. Policymakers might want to consider imposing a single reporting system to lessen the burden of and/or harmonize reporting obligations globally.

CONCLUSION

The emergence of security tokens and other crypto assets in recent years and the proliferation of Security Token Platforms for trading these assets necessitates the development of a sound legal and regulatory framework for post-trade processing of these securities. Using the post-trade processing responsibilities of today's FMIs as a guide, such responsibilities for Security Token Platforms should be promulgated in appropriate rules and regulations, assigned to an entity providing post-trade processing services – whether or not it is vertically integrated into the trading platform – and credibly enforced. Otherwise, a Security Token Platform cannot operate in a manner consistent with the public interest. Furthermore, unless their rules, regulations and best practices provide similar levels of safety, soundness and risk mitigation found in the current post-trade processing system for traditional securities, Security Token trading platforms will fail to attract participation by the institutional investment community, thereby constraining their growth and limiting their future role in the securities markets.

APPENDIX

THE CURRENT CLEARANCE AND SETTLEMENT FRAMEWORK FOR SECURITIES – TODAY'S POST-TRADE RESPONSIBILITIES

In the United States, DTCC subsidiaries The Depository Trust Company (DTC) and National Securities Clearing Corporation (NSCC) interoperate to provide post-trade clearance and settlement services for the U.S. equities markets. DTC is the world's largest securities depository and provides custody of securities certificates and other instruments, and settlement and asset services for eligible securities, including, among others, equities, warrants, rights, corporate debt and notes, municipal bonds, government securities, asset-backed securities, depositary receipts and money market instruments. DTC maintains securities accounts and settlement accounts for its participants (Participants), generally banks, broker-dealers and other financial institutions, including linked financial market infrastructures (FMIs). DTC holds eligible securities on behalf of Participants and reflects the transfer of interests in those securities among Participants by computerized book-entry.[48]

A DTC book-entry transfer may be a delivery free of payment (i.e., without a corresponding transfer of funds) or a delivery versus payment (DVP). DTC operates a DVP model 2 deferred net settlement system,[49] meaning that securities transfers are settled on a gross basis throughout the day, while the related funds transfers are settled on a net basis in central bank money at the end of the day. DTC processes book-entry transfers for institutional trades of its Participants that are affirmed and matched by an applicable settlement matching service.[50]

NSCC provides clearing, settlement, risk management, and central counterparty services for broker-to-broker trades involving equities, corporate and municipal debt, exchange-traded funds, and unit investment trusts in the United States. Securities whose trades are cleared and settled through NSCC and DTC and that are serviced by DTC are deposited with DTC as securities depository. When DTC credits interests in these securities to the securities accounts of Participants, those Participants acquire a beneficial interest in the securities.[51]

ENDNOTES

1 Hyperledger, an open-source collaborative effort created to advance cross-industry blockchain technologies, includes leaders in finance, banking, Internet of Things, supply chains, manufacturing and technology.

2 A "permissioned" blockchain system is one that is private, closed or restricted, whereby central authorities control which entities are permitted to join the network to participate.

3 A "crypto asset" is a digital asset which utilizes cryptography, peer-to-peer networking and a public ledger to regulate the creation of new units, verify transactions, and secure the transactions without the intervention of any middleman. A "token" for a crypto asset represents such asset on the network.

4 A "permissionless" blockchain system is one that is public, open and unrestricted, in which any entity with the requisite computer systems may participate.

5 This paper does not address the topic of whether and when an asset should be considered a security under any particular jurisdiction's laws.

6 Vertically integrated trading platforms are ones where trading and post-trade processing occur at the same legal entity. In most major securities markets around the world, vertically integrated platforms are less common than systems where one legal entity provides the trading venue and a separate entity, such as DTCC's subsidiaries in the U.S., provides the post-trade processing services.

7 In jurisdictions with developed capital markets, the supervision of securities-trading platforms is governed by statute and regulation, through which legal responsibilities are given to such platforms.

8 Note that, if deemed a commodity, a crypto asset referenced by a derivative contract that is listed and traded in the U.S. is subject to the Commodity Exchange Act and its implementing regulations.

9 See, for example, Templum Markets, LLC, which is a registered broker-dealer and operates an alternative trading system (ATS) and has petitioned the U.S. Securities and Exchange Commission (the "SEC") to issue a rulemaking on the clearance and settlement of security tokens.

10 While this paper focuses on Security Token Platforms, a functional approach to regulation might also be appropriate for DLT platforms in respect of other financial assets.

11 See Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions, Principles for Financial Market Infrastructures (2012) (hereinafter, the "PFMI Report").

12 See UK Gov't Office for Science, Distributed Ledger Technology: Beyond Block Chain, A Report by the UK Government Chief Scientific Adviser, at 5 (2016).

13 Several papers have summarized the basic components of a DLT structure. See Evangelos Benos et al., The Economics of Distributed Ledger Technology for Securities Settlement (2017); Committee on Payments and Market Infrastructures, Distributed Ledger Technology in Payment, Clearing and Settlement, An Analytical Framework (2017); FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (2017); David Mills et al., Distributed Ledger Technology in Payments, Clearing and Settlement (2016) (hereinafter, "Mills").

14 Whenever ownership of a security is referenced or "ledgered" on a blockchain, including a permissionless blockchain, DTCC would argue that, from a policy point of view, the question is raised as to whether settlement has been performed. This issue is discussed more fully below.

15 While the technology is evolving, there are some distributed database models where the ledger is not consensus based and as such, these technologies – akin to centralized databases – are not considered blockchain technology for purposes of this paper.

16 See supra notes 2 & 4.

17 Some companies offer technology solutions for discerning the identities of permissionless network users, but it is not certain that such solutions would ensure compliance with AML, KYC, or OFAC requirements.

18 See Mills, supra note 13, at 31.

19 It is conceivable that a known entity performs certain functions on a permissionless network such as the design of the protocols for smart contracts that run on a permissionless network. A permissionless network in this discussion means there is no known entity that controls who may join the network.

20 In the U.S., the PFMIs have been made applicable to certain entities providing post-trade processing for cash equities through the SEC's "Covered Clearing Agency Standards" at 17 C.F.R. § 240.17Ad-22(e) (2018).

21 Legal risk is defined for purposes of the PFMIs as the risk of the unexpected application of a law or regulation, usually resulting in a loss.

22 See Principle 1 of the PFMIs.

23 Section 8-110(a) of Article 8 provides that the local law of the issuer's jurisdiction governs, inter alia, the validity of a security, the rights and duties of the issuer with respect to registration of transfer of a security, and the effectiveness of registration of transfer of a security by the issuer. The issuer's jurisdiction is defined as the jurisdiction under which the issuer of the security is organized, or, if permitted by the law of that jurisdiction, the law of another jurisdiction specified by the issuer. Such jurisdictions would include both U.S. and non-U.S. jurisdictions.

24 81 Del. Laws. c. 86 (2017).

25 See Nat'l Conf. of State Legislatures, Blockchain State Legislation, http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx (last visited Jan. 30, 2019) (detailing proposed and enacted state blockchain legislation since 2015).

26 See Principle 2 of the PFMIs.

27 The exploitation of the coding flaw in the smart contracts comprising the Decentralized Autonomous Organization ("DAO") in 2016 is an example of an external attack on a permissionless network. Debate relating to the proposed correction of illegitimate trades resulting from the attack led to uncertainty and arguably negatively impacted confidence in the network.

28 See Principles 3 and 15 of the PFMIs.

29 Credit risk is defined for purposes of the PFMIs as the risk that a counterparty will be unable to meet fully its financial obligations when due or at any time in the future. Liquidity risk is defined for purposes of the PFMIs as the risk that a counterparty will have insufficient funds to meet its financial obligations as and when expected, although it may be able to do so in the future.

30 For example, the PFMIs provide that an FMI should maintain a viable recovery or orderly wind-down plan and should hold sufficient liquid net assets funded by equity to implement such plan. Notably, the SEC has largely adopted the language of Principle 15 and its key considerations from the PFMI Report into the Covered Clearing Agency Standards, supra note 20, with the SEC requiring that a covered clearing agency's plan for raising additional equity be updated annually.

31 See Principle 8 of the PFMIs.

32 See id.

33 For example, the U.S. Commodity Futures Trading Commission (the "CFTC") has provided guidance to the derivatives platforms the CFTC supervises concerning the number of blocks that must confirm a transfer of Bitcoin (BTC) between wallets before that transaction is considered final by the CFTC.

34 See Nancy Liao, On Settlement Finality and Distributed Ledger Technology, Notice & Comment (Jun. 9, 2017), http://yalejreg.com/nc/on-settlement-finality-and-distributed-ledger-technology-by-nancy-liao.

35 See e.g., 11 U.S.C. § 546(e) (2012); 12 U.S.C. § 1821(e)(8)(C) (2012).

36 See id.

37 See Principle 9 of the PFMIs.

38 See Fed. Reserve Banks of the Fed. Reserve Sys., Fedwire Securities Service Disclosure, at 69 (2017), available at https://www.frbservices.org/assets/financial-services/securities/securities-service-disclosure.pdf.

39 For example, in the U.S., if one of the platform components is a bank or a registered clearing agency designated as systemically important by the Financial Stability Oversight Council pursuant to the Payment, Clearing, and Settlement Supervision Act of 2010, it may be possible for the platform to have access to payment services at a Federal Reserve Bank. See 12 U.S.C. at § 5465(a).

40 See Principle 12 of the PFMIs.

41 See European Central Bank & Bank of Japan, Securities Settlement Systems: Delivery-versus-payment in a Distributed Ledger Environment, at 5 (2018).

42 Id. at 22.

43 See Principle 11 of the PFMIs relating to CSDs. See also Principle 16 of the PFMIs relating to custody risk and investment risk; the discussion in this section addresses only custody risk.

44 See Principle 17 of the PFMIs.

45 See Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures (2016).

46 In the U.S., the SEC's Regulation SCI (17 C.F.R. at § 242.1000 et seq.) requires SCI entities, which include stock and options exchanges, alternative trading systems and registered clearing agencies, to establish, maintain and enforce written policies and procedures reasonably designed to ensure that their, inter alia, securities clearance and settlement systems (i) have adequate levels of capacity, integrity, resiliency, availability and security and (ii) operate in a manner that complies with the Securities Exchange Act of 1934 (the "Exchange Act"), its implementing regulations, and the entity's own rules and governing documents. Regulation SCI also requires SCI entities to have and test business continuity and disaster recovery plans, including backup systems. Other cybersecurity standards include CPMI-IOSCO's Guidance on Cyber Resilience for Financial Market Infrastructures, supra note 48, and, in the U.S., the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool (see https://www.ffiec.gov/cyberassessmenttool.htm), against which U.S. FMIs are assessed, and the National Institute of Standards and Technology's voluntary Cybersecurity Framework (see https://www.nist.gov/cyberframework).

47 See Exchange Act Rule 17a-1, 17 C.F.R. at § 240.17a-1. Exchange Act Rule 17a-4(f), 17 C.F.R. at § 240.17a-4(f), provides a safe harbor allowing such records to be stored by means of "electronic storage media" but such safe harbor requires, among other things, that any data stored exclusively by means of an electronic storage medium be stored immutably in such medium, generally in a non-rewritable, non-erasable (write-once-read-many or WORM) format.

48 DTC facilitates asset servicing for securities it holds on behalf of Participants, including the processing and reporting of dividends and other distributions, shareholder voting and notices, and the processing of corporate actions such as stock splits and mergers. DTC facilitates announcement of corporate action events by collecting and validating corporate action information from the issuer or its agent and providing notice of the event to its Participants.

49 See PFMI Report, supra note 11, at Annex D.

50 Matching service providers include DTCC's subsidiary DTCC ITP LLC.

51 A Participant does not have a right to any particular security; each Participant has a proportionate interest in the fungible total inventory of the securities issue held by DTC.

ACKNOWLEDGMENTS

DTCC offers its gratitude to Arnold & Porter Kaye Scholer LLP for the firm's valuable input in shaping this paper.

Questions or comments about this white paper can be addressed to your DTCC Relationship Manager at DTCCClientCommunications@dtcc.com

14777PS032019